What Happens When CC Finds Memory Attacks

First, it is very important to note that memory alterations happen for a couple different reasons:

1. In-memory attacks
2. Interaction between programs
3. Software bugs
4. Exploits

So, a process injection or memory altering technique used, even between programs, is not necessarily a malicious action.

If a program which has suffered a likely malicious memory event (so, #1 or #4 above) is involved in an automated response by Cyber Crucible, an automated collection activity occurs.

The portion of memory that was altered in a program, as well as the “before” is saved to a structured Cyber Crucible format called .ccdiff

That injected or altered portion of memory is saved and is available for download in the Cyber Crucible web portal.

Why Is This Not Automatically Submitted to Virustotal (etc) for analysis?

In some circumstances, the malicious code that is used in an attack has variables which are unique to an attack, specifically to a victim.

Submitting this malicious code to a public analysis engine such as Virustotal would represent an undesired victim-identifying information disclosure to the security community.

Why Would Submitting This Binary Data to Virustotal (etc) be helpful?

Signature based antivirus and EDR tools look for strings or bytes of code seen in last attacks. Even if this malware has never been seen before, it may after a bit of time be known to the security community. These scanning tools usually do not need the code to be in a properly formatted binary to flag an association with a known piece of malware.

Revision #3
Created 2026-05-18 20:29:32 UTC by Dennis Underwood
Updated 2026-07-20 19:22:41 UTC by Dennis Underwood